(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 041 767 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
04.10.2000 Bulletin 2000/40

(51) Int Cl.[7]: **H04L 9/32**

(21) Application number: **99307624.9**

(22) Date of filing: **28.09.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **30.03.1999 JP 8823399**

(71) Applicant: **FUJITSU LIMITED**
Kawasaki-shi, Kanagawa 211-8588 (JP)

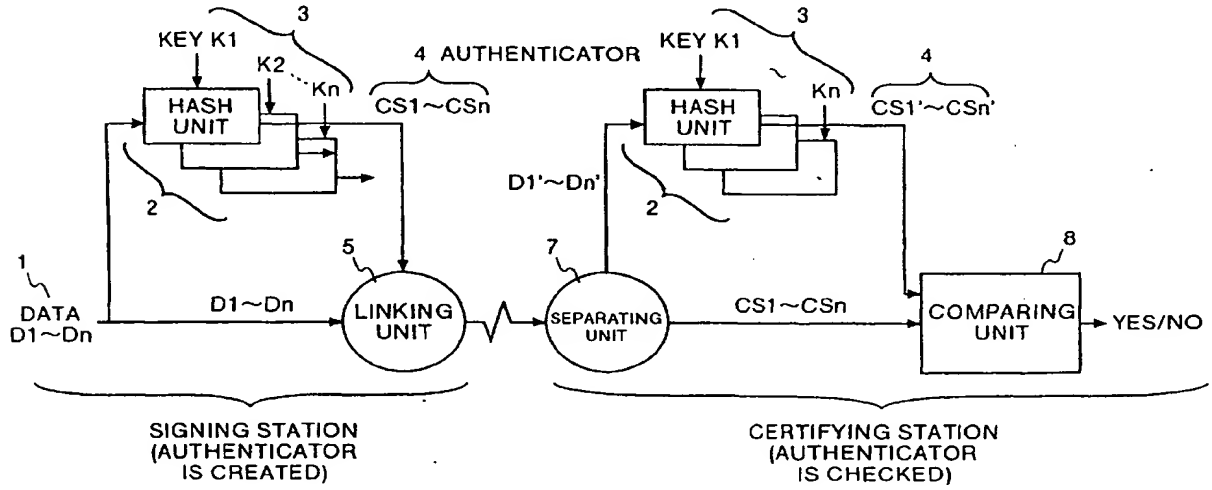
(72) Inventors:
- **Akiyama, Ryota**
  Nakahara-ku, Kawasaki-shi, Kanagawa 211 (JP)
- **Kotani, Seigo**
  Nakahara-ku, Kawasaki-shi, Kanagawa 211 (JP)
- **Hasebe, Takayuki**
  Nakahara-ku, Kawasaki-shi, Kanagawa 211 (JP)
- **Sasaki, Takaoki, c/o Fujitsu Basic Softeare Corp.**
  Tokyo 108-8531 (JP)

(74) Representative: **Stebbing, Timothy Charles et al**
Haseltine Lake & Co.,
Imperial House,
15-19 Kingsway
London WC2B 6UD (GB)

(54) Authentication of electronic data

(57) The authentication system has a signing station and a certifying station. The signing station divides the data to be transmitted into a plurality of blocks of data, a hash unit (2) creates a plurality of authenticators (4) by applying a different one-way function to each block. In the certifying station, a separating unit (7) divides the data into blocks, a hash unit (2) creates a plurality of authenticators (4) by applying a different one-way function to each block,and a comparing unit (8) compares the authenticators prepared anew with the authenticators separated from the received data and checks the authentication of the data from the comparison.

FIG.1



EP 1 041 767 A2

Description

[0001] The present invention relates to an authentication system, an authentication method, a signing apparatus/method, a certifying apparatus/method, a software program and a recording medium for the same for creating an authenticator by applying a one-way function to electronic data, appending a signature to the electronic data and checking authentication of the electronic data using the authenticator. The invention more particularly relates to prevention of forgery of the authenticator.

[0002] In association with recent development in the computer technology, there has increased an opportunity to accumulate electronic data such as a document prepared with characters, numerals, and strings of symbols in a database, or to transfer the data via a network. Considering these facts, how to avoid forgery of electronic data accumulated in a database or forgery of data during data communications has become a serious problem.

[0003] For solving the problem, there has been known an authentication technology in which an authenticator created by applying a one-way function to electronic data is appended thereto when the electronic data is transmitted and whether transmitted data is forged or not is verified using this authenticator when the electronic data is received.

[0004] More specifically, a station which transmits the electronic data (signing station) divides the electronic data into specified blocks, subjects the data to a signature processing by applying a one-way function such as a hash function to each of the divided data blocks, and transmits the data obtained through the processing to a distant station (certifying station). While a station which receives the electronic data creates an authenticator by applying a one-way function to a portion of the data other than the authenticator in the received electronic data, compares the created authenticator with the authenticator included in the electronic data, and verifies whether the electronic data has been forged or not.

[0005] However, even if the conventional technology described above is used, forgery of or tampering of electronic data can not possibly be verified if the portion of the authenticator itself is forged, namely if the signature is forged. Therefore, prevention of forgery of the signature becomes an issue that need to be resolved.

[0006] When a hash function is used, for example, it is possible to make more difficult to forgery of electronic data by making longer a processed block length of the hash function. However, it is not realistic to make the processed block length of the hash function extraordinarily long.

[0007] Especially, a conventional type of hash function is formed not based on an organized structural method but based on, in many cases, an empirical or an intuitive method obtained by combining a logical operation such as AND and OR with four rule of arithmetic in a complex manner. Therefore, enormous man power is required for experiments or the like when the block length of the hash function is to be increased.

[0008] Aspects of the present invention may provide, in view of the problem described above, an authentication system, an authentication method, a signing apparatus, a signing method, a certifying apparatus/method, a software program and a recording medium for the same which can efficiently prevent the forgery of the authenticator, when checking the authentication of the electronic data from an authenticator created using a one-way function.

[0009] In one aspect of the invention, a signing station creates a plurality of authenticators using a plurality of one-way functions then and links these plurality of authenticators to the electronic data, so that the length of the authenticators to be appended to the information can easily be made longer, which makes it possible to reduce a probability of misidentification of a forged authenticator.

[0010] The whole authenticator is not linked to the information, but only a portion of data obtained by truncating each of the authenticator is linked, which makes it more difficult for a third party to forge the authenticator.

[0011] A one-way operation is performed with the data using a different key, so that the length of the authenticators to be appended to the information can be made longer without utilizing a special one-way operation.

[0012] Authenticators can be discretely and independently prepared in parallel with each other, so that a plurality of authenticators can quickly be prepared.

[0013] Alternatively, an authenticator is prepared by utilizing intermediate data generated when a previous authenticator is created, so that generation of the authenticator is made more complicated, which makes it still difficult for a third party to forge the authenticator.

[0014] A signing station executes a step of preparing a plurality of authenticators by applying a different one-way function to each data, and a step of linking the created authenticators to the information, so that the length of the authenticators to be appended to the information can easily be made longer, which makes it possible to reduce a probability of misidentification of a forged authenticator.

[0015] In a method of the invention, there is a step of not linking the created whole authenticators to the information but linking only a portion of the data obtained by truncating each of the authenticators, which makes it more difficult for a third party to forge the authenticators.

[0016] Also, there is a step of performing a one-way operation with the data using a different key, so that the length of the authenticators to be appended to the information can be made longer without utilizing a special one-way operation.

[0017] Optionally, there are steps of discretely and independently creating the authenticators in parallel with each other, so that a plurality of authenticators can quickly be created.

[0018] As an alternative, there is a step of preparing the authenticator by utilizing an intermediate data generated when another authenticator is created, so that creation of the authenticator is made more complicated, which makes it still difficult for a third party to forge the authenticator.

[0019] In another aspect of the invention, a program stored in a recording medium makes a signing station execute a step of creating a plurality of authenticators by applying a different one-way function to each data, and a step of linking the created authenticators to the information, so that the length of the authenticators to be appended to the information can easily be made longer, which makes it possible to reduce a probability of misidentification of the forged authenticator.

[0020] Reference is made, by way of example, to the accompanying drawings in which:

Fig. 1 shows a system configuration of the authentication system used in an embodiment of the present invention;

Fig. 2A and Fig. 2B show more specific configurations (independent and multi-parallel configuration) of the authentication system shown in Fig. 1;

Fig. 3A and Fig. 3B show a case where the authentication system shown in Fig. 1 operates independently in three parallel branches;

Fig. 4A shows configuration and Fig. 4B shows operation when the hash units 2 perform parallel processing in association with each other;

Fig. 5 is a view showing one example of a document as an object for processing; and

Fig. 6A and Fig. 6B explain the safety in the authentication system used in the embodiment.

[0021] Detailed description is made hereinafter of a preferred embodiment of the present invention with reference to Fig. 1 to Fig. 6. It should be noted that this embodiment explains a case in which text data included in a document is the target data and an authenticator is created by applying a hash function to this target data.

[0022] Fig. 1 is a block diagram showing system configuration of the authentication system used in the embodiment of the present invention. In the left-hand side of Fig. 1 is a signature side (a signing station) which creates an authenticator by applying a hash function to the text data and links this authenticator to the text data before transmission. In the right-hand side of Fig. 1 is an authentication side (a certifying station) which creates an authenticator by applying a hash function to the data obtained by removing the authenticator from the received data, comparing the created authenticator with the authenticator included in the received data to check the correctness of the text data. Although it is assumed in this embodiment that a communication error will not occur in the process of transmission of data from the signing station to the certifying station. However, occurrence of error may be prevented by using an error-correction code or the like in some other cases.

[0023] At first, configuration of the signing station is described. As shown in Fig. 1, the signing station comprises a plurality of hash units 2 and keys 3, and a linking unit 5, and it is assumed that data 1 is input to this signing station.

[0024] The data 1 is text data as an object for transmission to the certifying station and consists of a plurality of data D1 to Dn obtained by dividing the data into data blocks of a size corresponding to a data length for a hash function. This data 1 is text data which contains numerals, characters, or symbols included in a document shown in Fig. 5, and, for example, "The present invention" shown in Fig. 5 corresponds to data D1.

[0025] The hash units 2 have one-way functions for converting the data D1 to Dn using keys K1 to Kn to authentication signs CS1 to CSn respectively, and they output the converted authentication signs CS1 to CSn to the linking unit 5. Although it is assumed that the hash units 2 perform processing corresponding to a known hash function in a protocol or the like for a method of verifying authentication signs based on the conventional technology, it is not always required that reverse conversion is ensured.

[0026] The keys 3 are the secret keys used when the hash units 2 perform scrambling of one-way data compression, and authentication signs 4 are prepared by the hash units 2 according to the keys K1 to Kn.

[0027] The linking unit 5 links the authenticators 4 created by the hash units 2 to data D1 to Dn that should originally be transmitted, and the linked authenticators 4 are appended, for example, to the end of the document as shown in Fig. 5.

[0028] Next, configuration of the certifying station is described. As shown in Fig. 1, the certifying station comprises a separating unit 7, a plurality of hash units 2 and keys 3, and a comparing unit 8, and data received from the signing station is input to the certifying station.

[0029] The separating unit 7 separates the data received from the signing station into data D1' to Dn' and the authentication signs 4. The data D1' to Dn' is inputted into the hash units 2, while the authenticators 4 are inputted into the comparing unit 8.

[0030] The comparing unit 8 compares the authentication signs separated from the received data with the authenticators created from the data D1' to Dn'. The comparing unit 8 certifies that the data is authentic when the authenticators are coincident with each other, and certifies that the data is forged one when the authenticators are not coincident.

[0031] As described above, the authentication system according to this embodiment is so configured that a signing station prepares a plurality of authenticators CS1 to CSn using a plurality of hash units, so that a data length of authenticators can be made longer, which makes it difficult to forge the authenticator by a third party.

[0032] A sequence of processing by the signing sta-

tion and the certifying station of the authentication system shown in Fig. 1 is described below.

(1) Creation of authenticators in the signature station:

[0033]

(1-1) The hash units 2 create CS1 to CSn each as the authenticators 4 by performing the processing of a one-way function using a key for each of input data D1 to Dn respectively into which the text data has been divided.

(1-2) The linking unit 5 links the authenticators CS1 to CSn created by the hash units 2 to the data D1 to Dn. As a result, for example, authenticators of 8 digits each consisting of 4 bits are appended, for example, to the end of the text as shown in the document of Fig. 5.

[0034] As described above, authenticators are created with a different key for each of the data D1 to Dn into which the text data has been divided, which makes it extremely difficult for a third party to forge the authenticator, thus reliability of text data being enhanced.

(2) Creation of authenticators in the certifying station:

[0035]

(2-1) The document shown in Fig. 5 prepared in the above step (1) is separated into the authenticators CS1 to Cn and data D1' to Dn' (data blocks).

(2-2) The hash units 2 create CS1' to CSn' as the authenticators 4 for the separated data D1' to Dn' respectively by using a different key.

(2-3) The created authenticators CS1' to CSn' are compared with the separated authenticators CS1 to CSn, and whether the authenticators are coincident with each other or not is determined. When the authenticators are coincident, then the text data is recognized as not being forged, namely as an authentic one. On the other hand, when even a single authenticator is not coincident, then the text data is recognized as being a forged one.

[0036] As described above, the certifying station creates authenticators CS1' to CSn' each with a different key for each of the data D1' to Dn' separated from received data, compares the created authenticators CS1' to CSn' with the authenticators CS1 to CSn which are separated from the received data, determines the text data as an authentic one when it is determined that all the authenticators are coincident with each other, on the other hand, determines the text data as a forged one when even one authenticator is not coincident.

[0037] More specific configuration (independent and multi-parallel configuration) of the authentication system shown in Fig. 1 is described. Fig. 2 is a block diagram showing more specific configuration (independent and multi-parallel configuration) of the authentication system shown in Fig. 1. Herein a case is assumed in which authenticators CS1 to CSn are created concurrently as well as in parallel from each of the input data D1 to Dn by using a different key.

[0038] Fig. 2A shows configuration of the authentication system, and in Fig. 2A, input data D1 to Dn is data D1 to Dn into which the text data as an object for transmission is divided. The hash units 2 create the authenticators CS using the keys K. More specifically, each of the hash units 2 consists of an EOR 21, a one-way function 22 such as a hash function, and a truncator 23.

[0039] The EOR 21 executes an operation of an exclusive OR, and operates herein an exclusive OR between the input data and a value obtained in the one-way function 22 in the previous time (an initial value IV is used for the first time).

[0040] The one-way function (corresponds to a one-way function device) 22 creates an irreversible authenticator CS with the help of the one-way function from the data processed in the EOR 21 based on the key K.

[0041] The truncator 23 truncates the authenticator CS prepared by the one-way function 22 and outputs the truncated authenticator. When the authenticator created by the one-way function 22 is outputted as it is, data length of the authenticator is naturally increased. However, an increase in the data length of the authenticator CS does not increase the safety of data but merely increases the amount of data to be transmitted.

[0042] Therefore, the truncator 23 truncates a portion of the authenticator created by the one-way function 22 so that increase in a data length of the authenticator CS is made really useful. Even if the authenticator is truncated, a symbol space same as that in the case where the authenticator are transmitted without being truncated is formed, therefore, security of data is not possibly reduced. Further, the security surely increases due to the truncation, because a third party will not know where the authenticator is truncated.

[0043] Output data (D1 to Dn, CS1 to CSn) is obtained, as shown in Fig. 5, by linking the created authenticators CS1 to CSn to input data D1 to Dn.

[0044] Fig. 2B shows how the authenticator CS is generated, and a portion of the left of Fig. 2B shows especially how the authenticator CS1 is generated.

[0045] In the left portion in Fig. 2B,

①"IV = Public constant" indicates that a public constant is set as the initial value IV which is inputted into the EOR 21 forming a part of the hash unit 2 in the far left side of Fig. 2A.

②"EK1[IV(+)D1]=L11" indicates that the EOR 21 in Fig. 2A operates an exclusive OR between the initial value IV set in① and the input data D1, and that the one-way function 22 performs a one-way operation (e.g., an operation by a hash function) with respect to the value obtained by operating the exclu-

sive OR using the key K1 to obtain a value L11.

③"EK1[L11(+)D2]=L12" indicates that the EOR 21 in Fig. 2A operates an exclusive OR between the value L11 obtained in② and the second input data D2, and that the one-way function 22 performs a one-way operation (e.g., an operation by a hash function) with respect to the value obtained by operating the exclusive OR using the key K1 to obtain a value L12.

④"EK1[L1(n-1)(+)Dn]=L1n" indicates that the EOR 21 in Fig. 2A operates, similarly as described above, an exclusive OR between the previously obtained value L1 (n-1) and n-th data Dn, and that the one-way function 22 performs a one-way operation (e.g., an operation by a hash function) with respect to the value obtained by operating the exclusive OR using the key K1 to obtain a value L1n.

⑤"Tr[L1n]=CS1" indicates that, when the operation is performed with respect to the last i.e. the n-th data Dn, a result of the last operation is outputted as the authenticator CS1.

[0046] Thus, the authenticator CS1 can be created by using the key 1 and initial value IV through the sequence of① to⑤ described above.

[0047] The central and the right portions of Fig. 2B respectively show, similarly to the sequence of① to⑤ in the left portion, sequence of computing the authenticators CS2 and CS3 respectively. By repeating the same operation, authenticators up to CSn can also be computed.

[0048] As described above, it is possible to concurrently compute authentication signs CS1 to CSn by using the keys K1 to Kn independently in n parallel branches. Herein, a forgery probability per CSn is $1/2^{np}$ (where p is a bit length of the authentication sign). This forgery probability can be reduced by increasing a number of authenticators CS. Even if a number of authenticators CS is increased, because the processing is in parallel, a time required for the processing does not change.

[0049] Next, a configuration as well as an operation is described when n=3 (independent triple-parallel configuration) in Fig. 2A and Fig. 2B with reference to Fig. 3A and Fig. 3B. Fig. 3A is a view showing a case where the authentication system shown in Fig. 1 operates independently in three parallel branches.

[0050] Fig. 3A shows configuration of a case where n in Fig. 2A is set to 3. The same reference numerals as those in Fig. 2A are assigned to the hash units 2, the EOR21, the one-way function 22, and the truncator 23, and detailed description thereof is omitted herein.

[0051] Fig. 3B shows how the authenticators CS1 to CS3 are generated in the hash units 2. Especially, the left portion of Fig. 3B shows a sequence of processing when the authenticator CS1 is created from the input data D1 to D3, the key K1, and initial value IV shown in Fig. 3A.

[0052] In the left portion in Fig. 3B,

①' "IV = Public constant" indicates that a public constant is set as the initial value IV which is inputted into the EOR 21 in the first hash unit 2 from the left side of Fig. 3A.

②' "EK1[IV(+)D1]=L11" indicates that the EOR 21 in Fig. 3A operates an exclusive OR between the initial value IV set in①' and the first input data D1, and that the one-way function 22 performs a one-way operation (e.g., an operation by a hash function) with respect to the value obtained by operating the exclusive OR using the key K1 to obtain a value L11.

③' "EK1[L11(+)D2]=L12" indicates that the EOR 21 in Fig. 3A operates an exclusive OR between the value L11 obtained in②' and the second input data D2, and that the one-way function 22 performs a one-way operation (e.g., an operation by a hash function) with respect to the value obtained by operating the exclusive OR using the key K1 to obtain a value L12.

④' "EK1[L12(+)D3]=L13" indicates that the EOR 21 in Fig. 3A operates, similarly as described above, an exclusive OR between the previously obtained value L12 and 3rd data D3, and that the one-way function 22 performs a one-way operation (e.g., an operation by a hash function) with respect to the value obtained by operating the exclusive OR using the key K1 to obtain a value L1n.

⑤' "Tr[L13]=CS1" indicates that, when the operation is performed with respect to the last i.e. 3rd data D3, a result of the 3rd operation is outputted as the authenticator CS1.

[0053] The central portion and the right portion of Fig. 3B respectively show, similarly to the sequence of①' to ⑤' in left portion, sequence of computing authenticators CS2 and CS3.

[0054] Through the above mentioned sequence of①' to⑤', it is possible to concurrently and independently compute authenticators CS1 to CS3 by using the keys K1 to K3 respectively.

[0055] A case has been explained above in which the hash units 2 perform parallel processing in three branches concurrently and independently. However, the present invention is not limited to this and it may be applied to a case in which the hash units 2 perform parallel processing in association with each other and not concurrently.

[0056] The case in which the hash units 2 perform parallel processing in association with each other is explained here. Fig. 4A shows configuration and Fig. 4B shows operation when hash units 2 perform parallel processing in association with each other. More specifically, these figures show a case in which n is set to 3 and intermediate data in a previous stage is used as an initial value in the next stage.

[0057] Fig. 4A shows configuration of a case where n is set to 3 and intermediate data in a previous stage is

used as the initial value in the next stage. The same reference numerals as those in Fig. 2A are assigned to the hash units 2, the EOR 21, the one-way function 22, and the truncator 23, and detailed description thereof is omitted herein.

[0058] This case is different from the case shown in Fig. 3A in that the initial value IV is set according to the intermediate data generated in other hash unit 2. The hash units 2 are so configured that as the initial value IV, intermediate data generated in other hash unit 2 is substituted. This configuration allows the authenticator CS to become more complicated, therefore, security is highly enhanced.

[0059] Fig. 4B shows how the authenticators CS1 to CS3 are generated in the hash units 2. Especially, the left portion of this figure shows a sequence of computing the authenticator CS1 in the hash unit 2 shown in the far left side of Fig. 4A. It should be noted that, the authenticator CS1 is computed through the same sequence as that from ① ' to ⑤ ' of the left portion in Fig. 3B, therefore, intermediate data generated in other hash unit 2 is not used.

[0060] The central portion in Fig. 4B shows a sequence of computing the authenticator CS2 in the hash unit 2 second from the left side in Fig. 4A. Herein, the authenticator CS2 is computed by using an intermediate result (L12) shown by arrow ⑥ obtained in the previous stage as the initial value through the same sequence as that from ① ' to ⑤ ' shown in the left portion of Fig. 3B. Namely, in this second hash unit 2, the intermediate data obtained in the first hash unit 2 is used.

[0061] The left portion of Fig. 4B shows a sequence of computing the authenticator CS3 in the hash unit 2 third from the left side in Fig. 4A. Herein, the authenticator CS3 is computed by using an intermediate result (L22) shown by arrow ⑦ obtained in the previous stage as the initial value through the same sequence as that from ① ' to ⑤ ' shown in the left portion of Fig. 3B. Namely, in this third hash unit 2, the intermediate data obtained in the second hash unit 2 is used.

[0062] Through the above mentioned sequence, the hash units 2 are configured so as not to independently compute the authenticators CS1 to CS3 but to compute them in association with each other. This configuration allows a sequence of creation of the authenticators CS1 to CS3 to become more complicated, therefore, it becomes more difficult for a third party to forge the text data.

[0063] Fig. 6A and Fig. 6B are conceptual views for explaining safety of the authentication system used in this embodiment. Fig. 6A shows the concept of the present invention while Fig. 6B shows the concept of the conventional technology.

[0064] In Fig. 6B, a text space M is a virtual space possibly occupied by the text as an object to be forged, and the authenticator space is a virtual space possibly occupied by the authenticator. When the text space M corresponds to the authenticator space one to one, it becomes necessary to increase the block length of the authenticator in order to make smaller a forged text space M2 on the text space M in the manner shown with the circle indicated by a dotted line to the circle indicated by a solid line, so that a probability that the forged authenticator is by mistake recognized as the genuine authenticator is reduced.

[0065] However, as the block length of the authenticator depends on the processing block length of a hash function, the block length of the authenticator cannot be easily made longer.

[0066] Therefore, in the present invention, as shown in Fig. 6A, a forged space is made smaller by making use of a plurality of keys, so that the probability that the forged authenticator is by mistake recognized as the genuine authenticator is reduced. More specifically, assuming in Fig. 6A that a forged-text space on the text space M when the key K1 is used is M1, that a forged text space on the text space M when the key K2 is used is M2, and that a forged text space on the text space M when the key K3 is used is M3, and when the keys K1, K2, and K3 according to the present invention are used, the space for forgery is a space for forgery M123 which is extremely small and it is the area commonly shared by the spaces for forgery M1, M2, and M3, thus a probability that the data can be forged becomes still smaller.

[0067] As described above, in the present invention, the signing station creates a plurality of authenticators using a plurality of one-way functions and then links these plurality of authenticators to the electronic data, while the certifying station compares the authenticators created from the electronic data which is separated from the received data with the authenticators included in this received data, and verifies whether the electronic data is a forged one or not. Therefore, with the present invention, even when the electronic data is a forged one, the probability of misidentification that the forged data may be erroneously recognized as an authentic data can greatly and easily be reduced, further, the probability of misidentification can be reduced through parallel processing without increasing the time required for preparing authenticators.

[0068] Furthermore, if the authenticator is truncated using a truncator, the probability of misidentification of a forged authenticator can further be reduced without increasing the amount of data required for the authenticator to be appended to the electronic data. In addition, intermediate data obtained when the authenticator is created in a previous stage is used as the initial value in the next stage, which allows the probability of misidentification to further be reduced.

[0069] The above description assumes that the object for processing is text data in a document. However, the present invention is not limited to the above case, but is also applicable to various types of multimedia data such as image data, video data, or audio data. In addition, although it has been described above that a hash function is used as a one-way function, the present invention

is not limited to the above case, and any one-way function other that the hash function may be used.

[0070] Although the invention has been described with respect to a specific embodiment for a complete and clear disclosure, the appended claims are not to be thus limited but are to be construed as embodying all modifications and alternative constructions that may occur to one skilled in the art which fairly fall within the basic teaching herein set forth.

Claims

1. An authentication system comprising:

   a signing station which creates an authenticator by applying a one-way function to information and then appends a signature generated from the authenticator to the information:
   a certifying station for checking the authentication of the information from the authenticator included in the data received from said signing station;

   wherein said signing station has,

   a first authenticator creating unit or dividing the information into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and
   a linking unit for linking the plurality of authenticators created in said first authenticator creating unit to the information;

   and said certifying station has,

   a separating unit for separating the information and the plurality of authenticators from the data received from said signing station;
   a second authenticator creating unit for dividing the information separated by said separating unit into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and
   a certifying unit for comparing the plurality of authenticators created by said second authenticator creating unit with the plurality of authenticators separated from the information by said separating unit, and checking the authentication of the information.

2. An authentication system according to Claim 1; wherein said linking unit links the authenticators obtained by truncating the authenticators created by said first authenticator creating unit to the information, and

   said certifying unit compares the authenticators obtained by truncating the authenticators created by said second authenticator creating unit to the authenticators separated from the information by said separating unit and checking the authentication of the information.

3. An authentication system according to Claim 2; wherein said first authenticator creating unit and said second authenticator creating unit create a first authenticator by subjecting first data to a one-way operation using a first key, and prepare a second authenticator by subjecting second data to a one-way operation using a second key.

4. An authentication system according to Claim 3; wherein each of said first authenticator creating unit and said second authenticator creating unit discretely and independently creates the first authenticator and the second authenticator in parallel with each other.

5. An authentication system according to Claim 3; wherein each of said first authenticator creating unit and said second authenticator creating unit utilize intermediate data when creating the second authenticator, which intermediate data is generated when the first authenticator is created.

6. An authentication method applied in an authentication system, wherein said authentication system has a signing station which creates an authenticator by applying a one-way function to information and then appends a signature generated from the authenticator to the information, and a certifying station for checking the authentication of the information from the authenticator included in the data received from said signing station; wherein

   said signing station executes,
   a first authenticator creating step of dividing the information into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and
   a transmitting step of linking the plurality of authenticators created in said first authenticator creating step to the information and transmitting the information to the certifying station; and
   said certifying station executes,
   a separating step of separating the information and the plurality of authenticators from the data received from said signing station;
   a second authenticator creating step of dividing the information separated in said separating step into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way

function to each of the data; and
a certifying step of comparing the plurality of authenticators created in said second authenticator creating step with the plurality of authenticators separated from the information in said separating step, and checking the authentication of the information.

7. An authentication method according to Claim 6; wherein said transmitting step comprises a step of linking the authenticators obtained by truncating the authenticators created in said first authenticator creating step to the information, and
said certifying step comprises a step of comparing the authenticator obtained by truncating the authenticators created in said second authenticator creating step to the authenticators separated from the information in said separating step and a step of checking the authentication of the information.

8. An authentication method according to Claim 7; wherein said first authenticator creating step and said second authenticator creating step comprise a step of creating a first authenticator by subjecting first data to a one-way operation using a first key, and a step of creating a second authenticator by subjecting second data to a one-way operation using a second key.

9. An authentication method according to Claim 8; wherein each of said first authenticator creating step and said second authenticator creating step comprise a step of discretely and independently creating the first authenticator and the second authenticator in parallel with each other.

10. An authentication system according to Claim 8; wherein each of said first authenticator creating step and said second authenticator creating step comprise a step of utilizing intermediate data when creating the second authenticator, which intermediate data is generated when the first authenticator is created.

11. A software program for making a computer execute an authentication method applied in an authentication system, wherein said authentication system has a signing station which creates an authenticator by applying a one-way function to information and then appends a signature generated from the authenticator to the information, and a certifying station for checking the authentication of the information from the authenticator included in the data received from said signing station; wherein

the program makes said signing station execute,
a first authenticator creating step of dividing the information into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and
a transmitting step of linking the plurality of authenticators created in said first authenticator creating step to the information and transmitting the information to the certifying station; and
the program makes said certifying station execute,
a separating step of separating the information and the plurality of authenticators from the data received from said signing station;
a second authenticator creating step of dividing the information separated in said separating step into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and
a certifying step of comparing the plurality of authenticators created in said second authenticator creating step with the plurality of authenticators separated from the information in said separating step, and checking the authentication of the information.

12. A signing apparatus which creates an authenticator by utilizing a key and applying a one-way function to information and then appends a signature to the information; said apparatus comprising:

a dividing unit for dividing the information into a plurality of data;
an authenticator creating unit for creating an authenticator by utilizing a key and applying a one-way function corresponding to each of the divided data; and
a linking unit for linking the plurality of created authenticators to the information.

13. A signing apparatus which creates an authenticator by utilizing a key and applying a one-way function to information and then appends a signature to the information; said apparatus comprising:

a dividing unit for dividing the information into a plurality of data;
an authenticator creating unit for repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to desired intermediate data for which the one-way function has already been applied as the next data; and
a linking unit for linking the plurality of created authenticators to the information.

14. A certifying apparatus which creates an authenticator by utilizing a key and applying a one-way function to information and then appends a signature to the information as well as checking the authentication of the information; said apparatus comprising:

a separating unit for separating information and the plurality of authenticators from the data;
a dividing unit for dividing the information into a plurality of data;
an authenticator creating unit for creating authenticators by utilizing a key and applying a one-way function corresponding to each of the divided data; and
a certifying unit for checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

15. A certifying apparatus which creates an authenticator by utilizing a key and applying a one-way function to information and then appends a signature to the information as well as checking the authentication of the information; said apparatus comprising:

a separating unit for separating information and the plurality of authenticators from the data;
a dividing unit for dividing the information into a plurality of data;
an authenticator creating unit for repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to desired intermediate data for which the one-way function has already been applied, as the next data; and
a certifying unit for checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

16. A software program for making a computer execute:

a dividing step of dividing information into a plurality of data;
an authenticator creating step of creating an authenticator by utilizing a key and applying a one-way function corresponding to each of the divided data; and
a linking step of linking the plurality of created authenticators to the information.

17. A software program for making a computer execute:

a dividing step of dividing information into a plurality of data;
an authenticator creating step of repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way function was applied; and
a linking step of linking the plurality of created authenticators to the information.

18. A software program for making a computer execute:

a separating step of separating information and a plurality of authenticators from data;
a dividing step of dividing the information into a plurality of data;
an authenticator creating step of creating authenticators by utilizing a key and applying a one-way function corresponding to each of the divided data; and
a certifying step of checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

19. A software program for making a computer execute:

a separating step of separating information and plurality of authenticators from data;
a dividing step of dividing the information into a plurality of data;
an authenticator creating step of repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way function was applied; and
a certifying step of checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

20. A signing method in which an authenticator is created by utilizing a key and applying a one-way function to information and then a signature is appended to the information; said method comprising:

a dividing step of dividing information into a plurality of data;
an authenticator creating step of creating authenticators by utilizing a key and applying a one-way function corresponding to each of the divided data; and
a linking step of linking the plurality of created authenticators to the information.

21. A signing method in which an authenticator is created by utilizing a key and applying a one-way function to information and then a signature is appended to the information; said method comprising:

a dividing step of dividing information into a plurality of data;
an authenticator creating step of repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way function was applied; and
a linking step of linking the plurality of created authenticators to the information.

22. A certifying method in which an authenticator is created by utilizing a key and applying a one-way function to information and then a signature is appended to the information as well as the authentication of the information is checked; said method comprising:

a separating step of separating information and a plurality of authenticators from data;
a dividing step of dividing the information into a plurality of data;
an authenticator creating step of creating authenticators by utilizing a key and applying a one-way function corresponding to each of the divided data; and
a certifying step of checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

23. A certifying method in which an authenticator is created by utilizing a key and applying a one-way function to information and then a signature is appended to the information as well as the authentication of the information is checked; said method comprising:

a separating step of separating information and plurality of authenticators from data;
a dividing step of dividing the information into a plurality of data;
an authenticator creating step of repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to desired intermediate data, for which the one-way function has been applied, as the next data; and
a certifying step of checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

24. A computer readable recording medium on which is recorded a software program according to any one of claims 11, 16, 17, 18 or 19.

FIG.1

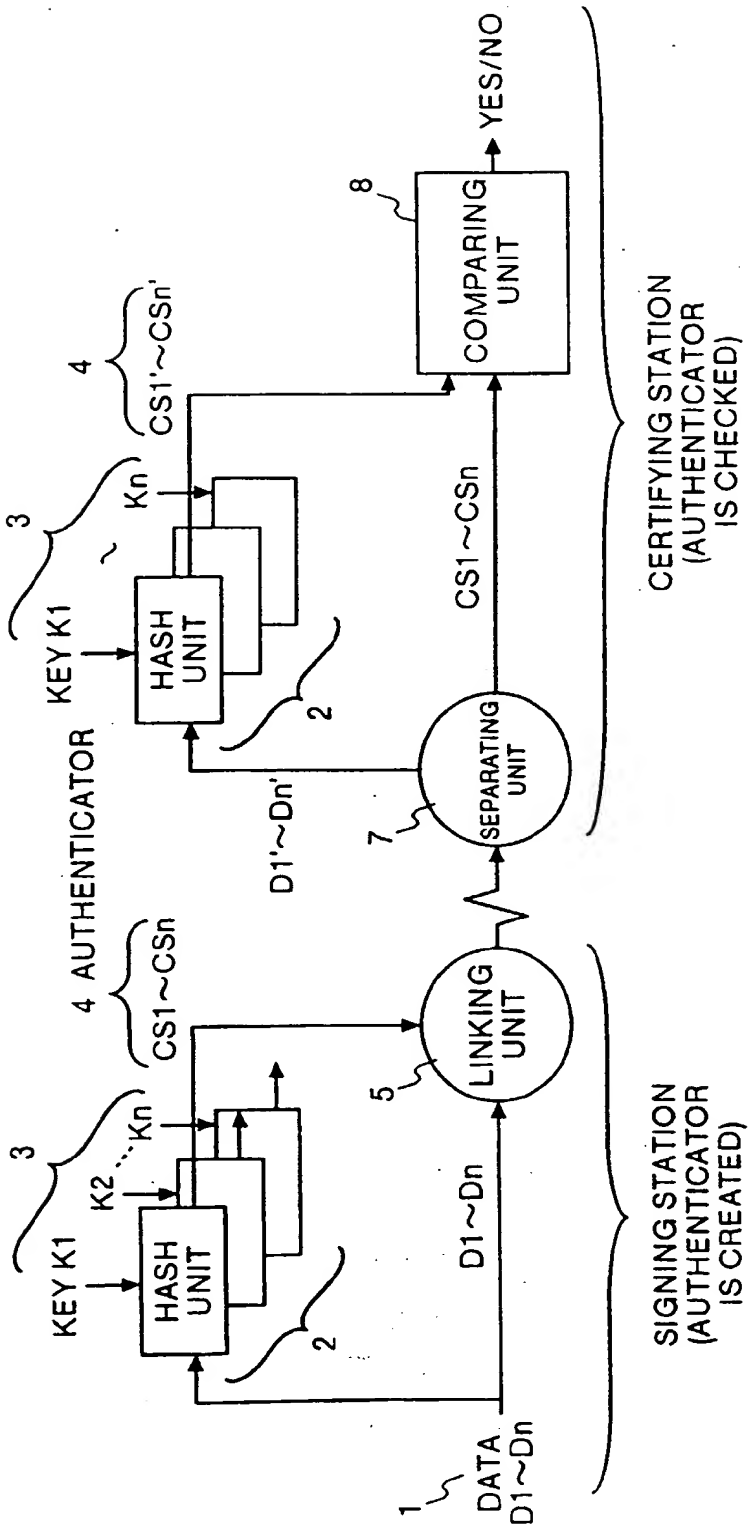

DATA D1~Dn
1
SIGNING STATION (AUTHENTICATOR IS CREATED)
CERTIFYING STATION (AUTHENTICATOR IS CHECKED)
4 AUTHENTICATOR
KEY K1
K2
Kn
HASH UNIT
2
3
CS1~CSn
4
CS1'~CSn'
D1~Dn
D1'~Dn'
LINKING UNIT
5
SEPARATING UNIT
7
COMPARING UNIT
8
YES/NO

FIG.2A

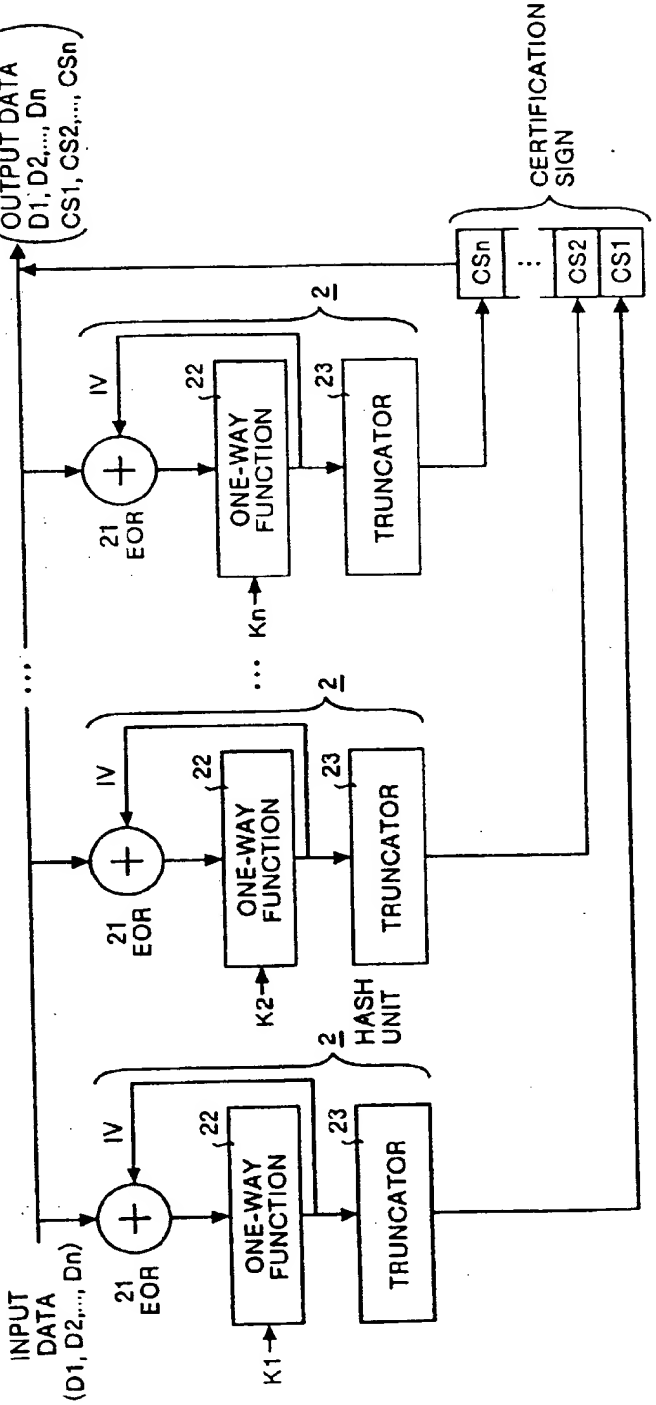


FIG.2B

(b-1)CS1-GENERATING PROCESS
①→IV=PUBLIC CONSTANT
②→EK1[IV(+)D1]=L11
③→EK1[L11(+)D2]=L12
. . . . . .
④→EK1[L1(n-1)(+)Dn]=L1n
⑤→Tr[L1n]=CS1

(b-2)CS2-GENERATING PROCESS
IV=PUBLIC CONSTANT
EK2[IV(+)D1]=L21
EK2[L21(+)D2]=L22
. . . . . .
EK2[L2(n-1)(+)Dn]=L2n
Tr[L2n]=CS2

(b-3)CS3-GENERATING PROCESS
IV=PUBLIC CONSTANT
EK3[IV(+)D1]=L31
EK3[L31(+)D2]=L32
. . . . . .
EK3[L3(n-1)(+)Dn]=L3n
Tr[L3n]=CS3

FIG.3A

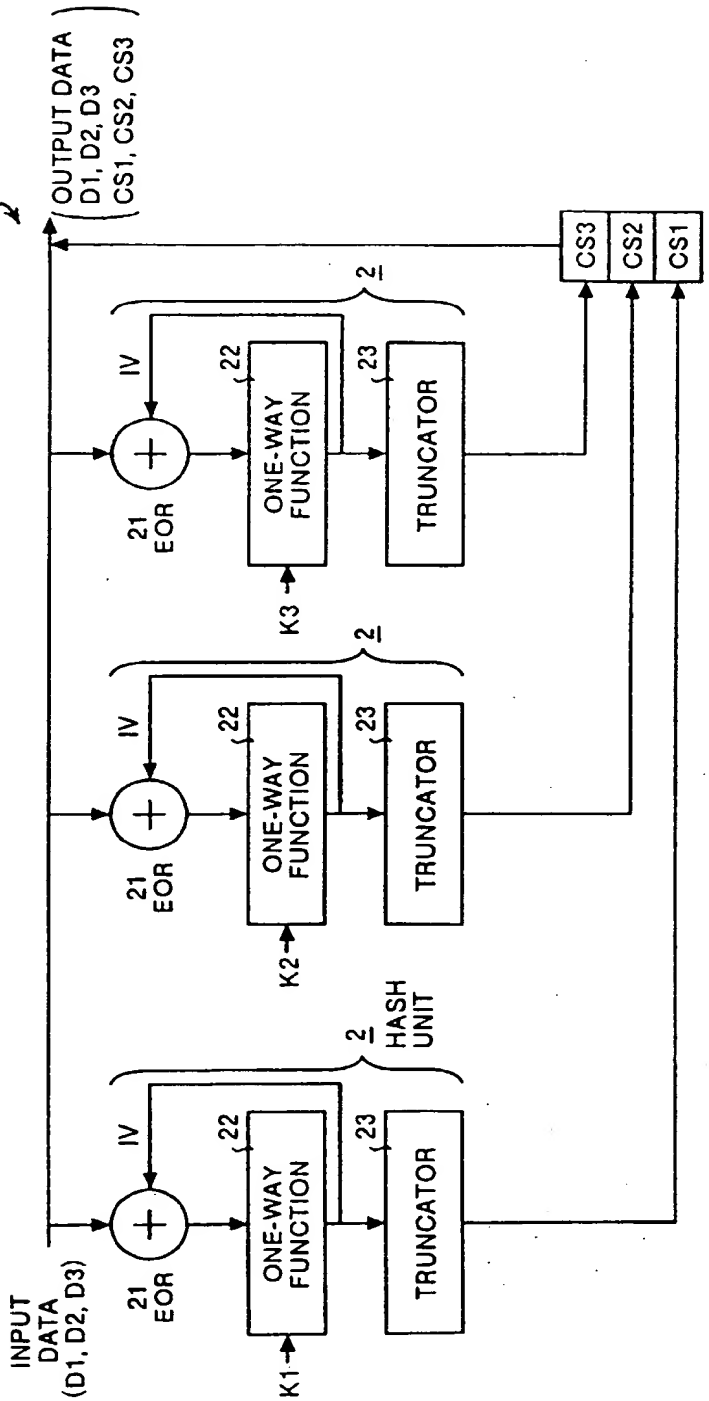


FIG.3B

(b-1)CS1-GENERATING PROCESS
①→IV=PUBLIC CONSTANT
②→EK1[IV(+)D1]=L11
③→EK1[L11(+)D2]=L12
④→EK1[L12(+)D3]=L13
⑤→Tr[L13]=CS1

(b-2)CS2-GENERATING PROCESS
IV=PUBLIC CONSTANT
EK2[IV(+)D1]=L21
EK2[L21(+)D2]=L22
EK2[L22(+)D3]=L23
Tr[L23]=CS2

(b-3)CS3-GENERATING PROCESS
IV=PUBLIC CONSTANT
EK3[IV(+)D1]=L31
EK3[L31(+)D2]=L32
EK3[L32(+)D3]=L33
Tr[L33]=CS3

FIG.4A

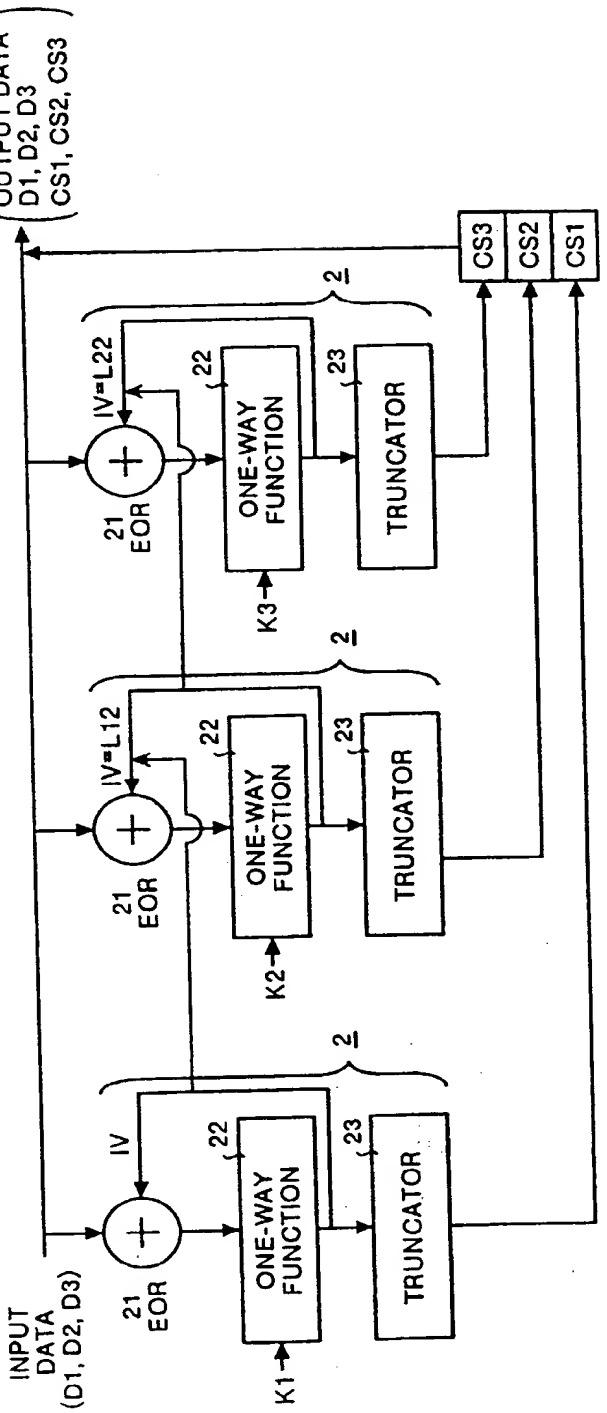

2
OUTPUT DATA
D1, D2, D3
CS1, CS2, CS3
INPUT
DATA
(D1, D2, D3)
IV
IV=L12
IV=L22
21
EOR
22
ONE-WAY
FUNCTION
23
TRUNCATOR
K1
K2
K3
CS3
CS2
CS1

FIG.4B

(b-1)CS1-GENERATING PROCESS
IV=PUBLIC CONSTANT
EK1[IV(+)D1]=L11
EK1[L11(+)D2]=L12
EK1[L12(+)D3]=L13
Tr[L13]=CS1
⑥
(b-2)CS2-GENERATING PROCESS
IV=L12
EK2[IV(+)D1]=L21
EK2[L21(+)D2]=L22
EK2[L22(+)D3]=L23
Tr[L23]=CS2
⑦
(b-3)CS3-GENERATING PROCESS
IV=L22
EK3[IV(+)D1]=L31
EK3[L31(+)D2]=L32
EK3[L32(+)D3]=L33
Tr[L33]=CS3

FIG.5

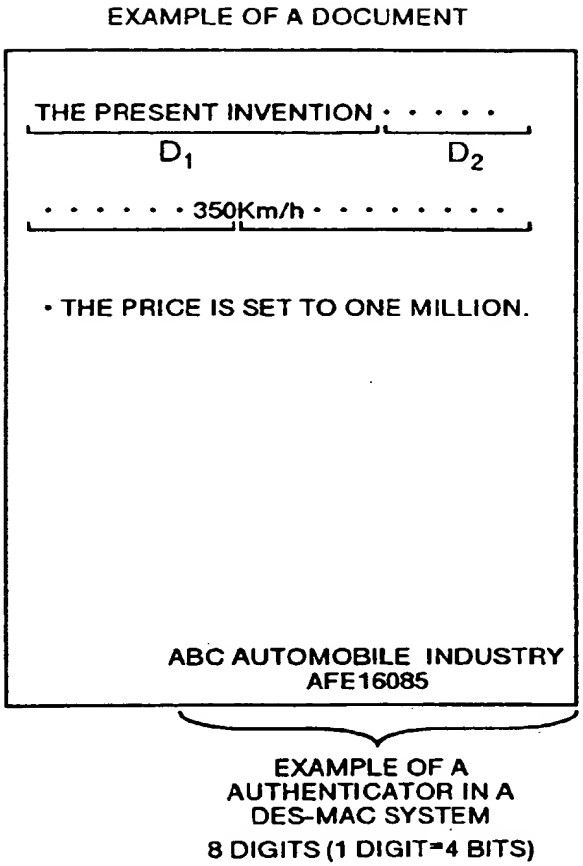

EXAMPLE OF A DOCUMENT
THE PRESENT INVENTION · · · · ·
D1
D2
· · · · · · 350Km/h · · · · · · · ·
· THE PRICE IS SET TO ONE MILLION.
ABC AUTOMOBILE INDUSTRY
AFE16085
EXAMPLE OF A
AUTHENTICATOR IN A
DES-MAC SYSTEM
8 DIGITS (1 DIGIT=4 BITS)

FIG.6A

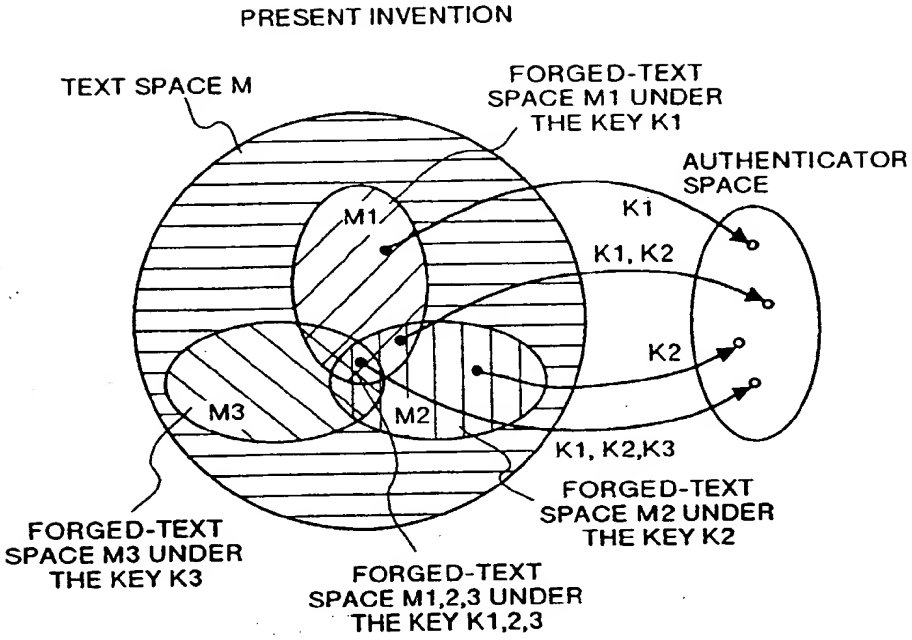
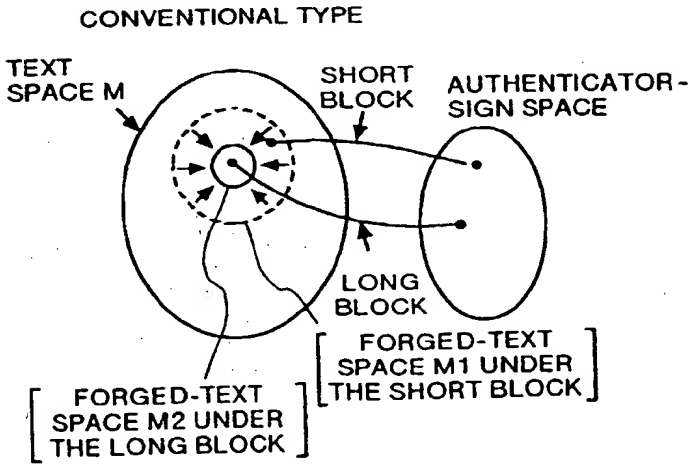

PRESENT INVENTION
TEXT SPACE M
FORGED-TEXT SPACE M1 UNDER THE KEY K1
AUTHENTICATOR SPACE
M1
K1
K1, K2
K2
M3
M2
K1, K2,K3
FORGED-TEXT SPACE M2 UNDER THE KEY K2
FORGED-TEXT SPACE M3 UNDER THE KEY K3
FORGED-TEXT SPACE M1,2,3 UNDER THE KEY K1,2,3

FIG.6B


CONVENTIONAL TYPE
TEXT SPACE M
SHORT BLOCK
AUTHENTICATOR-SIGN SPACE
LONG BLOCK
FORGED-TEXT SPACE M1 UNDER THE SHORT BLOCK
FORGED-TEXT SPACE M2 UNDER THE LONG BLOCK

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 041 767 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
15.05.2002 Bulletin 2002/20

(43) Date of publication A2:
04.10.2000 Bulletin 2000/40

(21) Application number: **99307624.9**

(22) Date of filing: **28.09.1999**

(51) Int Cl.[7]: **H04L 9/32**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **30.03.1999 JP 8823399**

(71) Applicant: **FUJITSU LIMITED**
Kawasaki-shi, Kanagawa 211-8588 (JP)

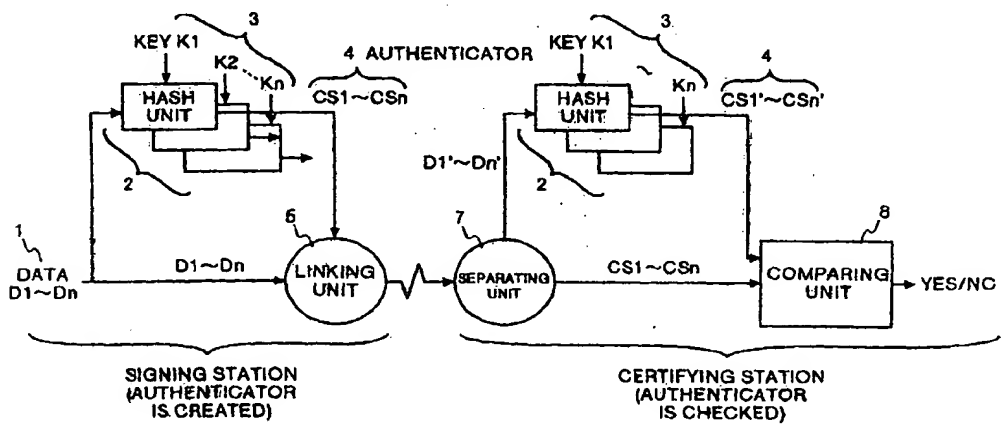
(72) Inventors:
- **Akiyama, Ryota**
  Nakahara-ku, Kawasaki-shi, Kanagawa 211 (JP)
- **Kotani, Seigo**
  Nakahara-ku, Kawasaki-shi, Kanagawa 211 (JP)
- **Hasebe, Takayuki**
  Nakahara-ku, Kawasaki-shi, Kanagawa 211 (JP)
- **Sasaki, Takaoki, c/o Fujitsu Basic Softeare Corp.**
  Tokyo 108-8531 (JP)

(74) Representative: **Stebbing, Timothy Charles et al**
Haseltine Lake & Co.,
Imperial House,
15-19 Kingsway
London WC2B 6UD (GB)

(54) Authentication of electronic data

(57) The authentication system has a signing station and a certifying station. The signing station divides the data to be transmitted into a plurality of blocks of data, a hash unit (2) creates a plurality of authenticators (4) by applying a different one-way function to each block. In the certifying station, a separating unit (7) divides the data into blocks, a hash unit (2) creates a plurality of authenticators (4) by applying a different one-way function to each block,and a comparing unit (8) compares the authenticators prepared anew with the authenticators separated from the received data and checks the authentication of the data from the comparison.

FIG.1



EP 1 041 767 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 30 7624

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X Y	EP 0 781 003 A (GEN INSTRUMENT CORP) 25 June 1997 (1997-06-25) * column 3, line 49 - column 4, line 42 * * column 8, line 31 - column 9, line 35 * * column 10, line 43 - column 11, line 34 * * figures 1-3 *	1,2,6,7, 11-24 3-5,8-10	H04L9/32
X A	US 5 768 382 A (JORASCH JAMES ET AL) 16 June 1998 (1998-06-16) * column 17, line 64 - column 19, line 19 * * figures 6A,6B *	1,2,6,7, 11 3-5,8-10	
A	US 5 757 919 A (DAVIS DEREK L ET AL) 26 May 1998 (1998-05-26) * column 2, line 54 - column 3, line 8 * * column 4, line 43 - column 5, line 20 * * column 6, line 21 - line 30 * * claim 8 *	2	
A	WO 99 07149 A (SCIENTIFIC ATLANTA) 11 February 1999 (1999-02-11) * claim 3 *	2	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04L H04N
Y	EP 0 822 720 A (THOMSON MULTIMEDIA SA) 4 February 1998 (1998-02-04) * column 6, line 51 - column 7, line 53 * * column 10, line 2 - line 31 * * figures 3B,5 *	3-5,8-10	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	20 March 2002	Dujardin, C

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 30 7624

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

20-03-2002

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
EP 0781003	A	25-06-1997	US	5754659	A	19-05-1998
			AU	713597	B2	09-12-1999
			AU	7043096	A	26-06-1997
			CA	2184946	A1	23-06-1997
			EP	0781003	A2	25-06-1997
			JP	9200199	A	31-07-1997
			NO	963626	A	23-06-1997
US 5768382	A	16-06-1998	AU	1081997	A	11-06-1997
			EP	0862824	A1	09-09-1998
			JP	2001526550	T	18-12-2001
			WO	9719537	A1	29-05-1997
			US	5970143	A	19-10-1999
			US	2002010013	A1	24-01-2002
US 5757919	A	26-05-1998	AU	5688998	A	03-07-1998
			DE	19782169	C2	06-09-2001
			DE	19782169	T0	28-10-1999
			GB	2334866	A ,B	01-09-1999
			JP	2001508893	T	03-07-2001
			WO	9826535	A1	18-06-1998
WO 9907149	A	11-02-1999	AU	1581699	A	08-03-1999
			AU	8670598	A	22-02-1999
			AU	8679798	A	22-02-1999
			AU	8679898	A	22-02-1999
			AU	8764298	A	22-02-1999
			AU	8823398	A	22-02-1999
			AU	8823698	A	22-02-1999
			BR	9810966	A	20-11-2001
			BR	9810967	A	30-10-2001
			BR	9815606	A	22-01-2002
			BR	9815607	A	13-11-2001
			DE	69802288	D1	06-12-2001
			DE	69802540	D1	20-12-2001
			EP	1189438	A2	20-03-2002
			EP	1189439	A2	20-03-2002
			EP	1010323	A1	21-06-2000
			EP	1010324	A1	21-06-2000
			EP	1010325	A1	21-06-2000
			EP	1013091	A1	28-06-2000
			EP	1000508	A1	17-05-2000
			EP	1000509	A1	17-05-2000
			EP	1000511	A2	17-05-2000
			JP	2001513587	T	04-09-2001
			JP	2001512842	T	28-08-2001

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 30 7624

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

20-03-2002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9907149 A		WO 9907145 A1	11-02-1999
		WO 9907146 A1	11-02-1999
		WO 9907147 A1	11-02-1999
		WO 9907148 A1	11-02-1999
		WO 9907149 A1	11-02-1999
		WO 9909743 A2	25-02-1999
		WO 9907150 A1	11-02-1999
		US 6105134 A	15-08-2000
		US 6292568 B1	18-09-2001
		US 6252964 B1	26-06-2001
		US 2001001014 A1	10-05-2001
		US 2001046299 A1	29-11-2001
		US 2001053226 A1	20-12-2001
		US 6246767 B1	12-06-2001
EP 0822720 A	04-02-1998	FR 2751817 A1	30-01-1998
		CN 1175142 A	04-03-1998
		EP 0822720 A1	04-02-1998
		JP 10098462 A	14-04-1998
		US 6091818 A	18-07-2000

EPO FORM P0459